Discrete Mathematics 309 (2009) 606–612

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

On set systems with restricted intersections modulo p and p-ary t-designs

Richard M. Wilson

Department of Mathematics 253–37, California Institute of Technology, Pasadena, CA 91125, USA

ARTICLE INFO

Article history:
Received 13 November 2007
Accepted 12 September 2008
Available online 23 October 2008

Keywords:
t-designs
Incidence matrices
Extremal set theory
Set intersections

ABSTRACT

We consider bounds on the size of families $\mathcal{F}$ of subsets of a v-set subject to restrictions modulo a prime p on the cardinalities of the pairwise intersections. We improve the known bound when $\mathcal{F}$ is allowed to contain sets of different sizes, but only in a special case. We show that if the bound for uniform families $\mathcal{F}$ holds with equality, then $\mathcal{F}$ is the set of blocks of what we call a p-ary t-design for certain values of t. This motivates us to make a few observations about p-ary t-designs for their own sake.

1. Introduction

The following theorem was proved in [3].

Theorem 1. *Let p be a prime and $k, \mu_1, \mu_2, \ldots, \mu_s$ integers that are distinct modulo p. If $\mathcal{F}$ is a family of k-subsets of a v-set X such that*

$$|A \cap B| \equiv \text{one of } \mu_1, \mu_2, \ldots, \mu_s \pmod{p}$$

for all distinct $A, B \in \mathcal{F}$, then

$$|\mathcal{F}| \le \binom{v}{s}.$$

The case "$p = 0$" of this theorem, when congruence is replaced by equality, is from [7]. Ph. Delsarte showed in [2] that equality in Theorem 1 in the "$p = 0$" case implies that $(X, \mathcal{F})$ is a t-design (see below for the definition) with $t = 2s$. We will give a form of this result (in Theorem 5) which applies to the case of equality in Theorem 1 in general, as well as to the case of equality in Theorem 2.

We remark that P. Frankl has described some simple but nontrivial examples where equality holds in Theorem 5. Suppose there exists an s-$(v, k+s, 1)$ design $(X, \mathcal{B})$ with $k > 2s$. Let $\mathcal{F}$ consist of all k-subsets A that are contained in some block B of $\mathcal{B}$. Sets $A_1, A_2 \in \mathcal{F}$ meet in at least $k-s$ points if they are in the same block of the design, and at most $s-1$ points if they are contained in different blocks (which intersect in at most $s-1$ points as any s-subset is contained in exactly one block B). So the hypothesis of Theorem 1 holds with $\mu_1, \mu_2, \ldots, \mu_s = 0, 1, \ldots, s-1$ when p is any prime divisor of $k-s$ with $p > s$. Whether there is such a prime p or not, a simple calculation shows that $|\mathcal{F}| = \binom{v}{s}$.

The results in [3] can be extended to the theorem below. See [1,4]. By an *integer-valued* polynomial, we mean a polynomial $f(x)$ that takes integer values for all integers x. Equivalently, $f(x)$ is an integer linear combination of the polynomials $\binom{x}{0}, \binom{x}{1}, \binom{x}{2}, \ldots$.

E-mail address: rmw@caltech.edu.

0012-365X/$ – see front matter © 2009 Published by Elsevier B.V.
doi:10.1016/j.disc.2008.09.025

Theorem 2. *Let v and k be positive integers and p a prime. Suppose that $f(x)$ is an integer-valued polynomial of degree s and $\mathcal{F}$ a family of k-subsets of a v-set such that $f(k) \not\equiv 0 \pmod p$, but*

$$f(|A \cap B|) \equiv 0 \pmod p$$

for every pair A, B of distinct members of $\mathcal{F}$. Then

$$|\mathcal{F}| \le \binom{v}{s}. \tag{1}$$

Theorem 2 implies Theorem 1 when we take

$$f(x) = (x - \mu_1)(x - \mu_2) \cdots (x - \mu_s).$$

If not all sets in $\mathcal{F}$ in the statement of Theorem 2 have the same cardinality, but $f(|A|) \not\equiv 0 \pmod p$ for every $A \in \mathcal{F}$, then one can still prove

$$|\mathcal{F}| \le \binom{v}{s} + \binom{v}{s-1} + \cdots + \binom{v}{1} + \binom{v}{0}. \tag{2}$$

See [1] and below (Section 2).

One purpose of this paper is to improve this bound from (2) to (1) in the case where the sets in $\mathcal{F}$ are not necessarily of the same size, but their sizes are all congruent to some integer ℓ modulo p.

Theorem 3. *Let v be a positive integer, ℓ any integer, and p a prime. Suppose that $f(x)$ is an integer-valued polynomial of degree s, $s < p$, and that $f(\ell) \not\equiv 0 \pmod p$. Let $\mathcal{F}$ be a family of subsets of a v-set X such that $|A| \equiv \ell \pmod p$ for every $A \in \mathcal{F}$ and where*

$$f(|A \cap B|) \equiv 0 \pmod p$$

for every pair A, B of distinct members of $\mathcal{F}$. Then

$$|\mathcal{F}| \le \binom{v}{s}. \tag{3}$$

We remark that when $s = 1$ and $f(x) = x - \mu$, examples of families with nonconstant set size that satisfy Theorem 3 with equality are provided by the "λ-designs" of Ryser and Woodall. These have two set sizes k_1 and k_2, that sum to $v + 1$; distinct sets meet in a sets of constant size μ, say. The prime p may be any prime divisor of $k_2 - k_1$ that does not divide $k_1 - \mu$ (if any).

Theorem 3 will be proved in Section 2. We give two lemmas in that section which are necessary for the proof and also are needed for the results of Sections 4 and 5.

In particular, Theorem 3 has the following corollary.

Corollary 4. *Let v be a positive integer, ℓ any integer, and let p be a prime. Suppose $\mathcal{F}$ is a family of subsets of a v-set so that $|A| \equiv \ell \pmod p$ for every $A \in \mathcal{F}$ but $|A \cap B| \not\equiv \ell \pmod p$ for all distinct $A, B \in \mathcal{F}$. Then*

$$|\mathcal{F}| \le \binom{v}{p-1}.$$

Given a multiset $\mathcal{A}$ of subsets of a set X, let $\lambda(T)$ denote the number of members of $\mathcal{A}$ that contain T, counting each subset $A \in \mathcal{A}$ according to its multiplicity. It will be convenient to use λ in this way while also using it to denote an integer.

A *classical* t-(v, k, λ) *design* consists of a v-set X and a set (or more generally a multiset) $\mathcal{A}$ of k-subsets (called blocks) of X so that $\lambda(T) = \lambda$ for every t-subset T of X. Any family of k-subsets is a 0-design.

Let p be a prime. We will use the term *p-ary* t-(v, k, λ) *design* for a v-set X and a multiset $\mathcal{A}$ of k-subsets (called blocks) of X so that $\lambda(T) \equiv \lambda \pmod p$ for every t-subset T of X.

It is well known that a classical t-design is also a j-design for $j = 0, 1, 2, \ldots, t$. But it is not true that a p-ary t-design is necessarily a j-design for all $j \le t$; see Section 4. By a *p-ary S-design*, we mean a set system $(X, \mathcal{A})$ which, for every $t \in S$, is a t-(v, k, λ_t) design for some λ_t. A classical t-design is a p-ary $\{0, 1, 2, \ldots, t\}$-design for every p. The following theorem will be proved in Section 3.

Theorem 5. *Let v be a positive integer and p a prime. Suppose that $f(x)$ is an integer-valued polynomial of degree s, $s < p$, and that $f(k) \not\equiv 0 \pmod p$. Let $\mathcal{F}$ be a family of k-subsets of a v-set X such that*

$$f(|A \cap B|) \equiv 0 \pmod p$$

for every pair A, B of distinct members of $\mathcal{F}$. If $|\mathcal{F}| = \binom{v}{s}$, then $\mathcal{F}$ is the set of blocks of a p-ary $\{s, s+1, \ldots, 2s\}$-design on point set X.

We make a few observations on p-ary t-designs for their own sake. In Section 4, we give necessary and sufficient conditions for the existence of p-ary t-designs and also consider p-ary t-designs that are not p-ary s-designs. In Section 5 we discuss Fisher-like inequalities on the number of blocks of p-ary t-designs.

2. Two lemmas and the proof of Theorem 3

The rank of an integer matrix M when considered as a matrix over the field F_p of p elements (i.e. modulo p) will be called the p-rank of M. This is the dimension of $\mathrm{row}_p(M)$, the row space of M over F_p.

Given matrices M_1 and M_2 with the same number of columns, we use $M_1 \sqcup M_2$ to denote the matrix

$$\begin{array}{|c|}\hline M_1 \\ \hline M_2 \\ \hline \end{array}$$

whose row set is the union of those of the two matrices (the order of the rows is not important).

Given a family $\mathcal{F}$ of b subsets of a v-set X, define the *inclusion matrices* $N_0, N_1, N_2, \ldots$ as follows. The rows of the $\binom{v}{i}$ by b matrix N_i are to be indexed by the i-subsets of X and the columns by the members of $\mathcal{F}$. The entry in row I and column A is to be

$$N_i(I, A) = \begin{cases} 1 & \text{if } I \subseteq A, \\ 0 & \text{otherwise.} \end{cases}$$

Note that the entry in row A and column B of $N_i^\top N_i$ is the sum over all i-subsets I of $N_i(I, A)N_i(I, B)$, which is the number $\binom{|A\cap B|}{i}$ of i-subsets contained in both A and B.

Assume that the hypotheses of Theorem 3 hold. Write

$$f(x) = c_0 + c_1\binom{x}{1} + c_2\binom{x}{2} + \cdots + c_s\binom{x}{s}$$

for some integer coefficients c_i. Since the degree of $f(x)$ is less than p, $f(a) \equiv f(b) \pmod p$ whenever $a \equiv b \pmod p$. Consider the matrix

$$P = c_0N_0^\top N_0 + c_1N_1^\top N_1 + c_2N_2^\top N_2 + \cdots + c_sN_s^\top N_s. \tag{4}$$

The entry in row A and column B of P is $f(|A \cap B|)$, and this is 0 modulo p if $A \neq B$, i.e. off the diagonal, while the diagonal entries of P are congruent to $f(\ell) \not\equiv 0 \pmod p$. Thus P is nonsingular modulo p, and hence nonsingular over the rationals.

Whether we work over the rationals or over F_p, the row space of $N_i^\top N_i$ is contained in the row space of N_i, so the the row space of P is contained in the sum U of the row spaces of $N_0, N_1, \ldots, N_s$. The rank $|\mathcal{F}|$ of P cannot exceed the dimension of U, which is at most $1 + v + \cdots + \binom{v}{s}$.

When all members of $\mathcal{F}$ have the same size k, the row spaces over the rationals of $N_0, N_1, \ldots, N_s$ are contained in the row space of N_s; see (6) below. It is not necessarily true that the row spaces over F_p of $N_0, N_1, \ldots, N_s$ are contained in $\mathrm{row}_p(N_s)$. However, Lemma 7 below shows that as long as all sets in $\mathcal{F}$ have sizes $\equiv \ell \pmod p$ and $s < p$, the row spaces modulo p of $N_0, N_1, \ldots, N_s$ are all contained in $\mathrm{row}_p(L)$ for a certain integer matrix L with $\binom{v}{s}$ rows. Once Lemma 7 is proved, we see that the p-rank of P cannot exceed $\binom{v}{s}$, and the proof of Theorem 3 will be complete.

We use W_{ij} for the $\binom{v}{i}$ by $\binom{v}{j}$ matrix which is the i-th inclusion matrix for the family of j-subsets of X, $0 \le i \le j \le v$.

Lemma 6. *Let v and k be given. For $j = 0, 1, \ldots, \min\{k, v-k\}$, there exists a matrix E_{jk} that consists of $\binom{v}{j} - \binom{v}{j-1}$ rows of W_{jk} such that for any $t \le \min\{k, v-k\}$, (i) the $\binom{v}{t}$ by $\binom{v}{k}$ matrix*

$$\bigsqcup_{j=0}^{t} E_{jk} = \begin{array}{|c|}\hline E_{0k} \\ \hline E_{1k} \\ \hline E_{2k} \\ \hline \vdots \\ \hline E_{tk} \\ \hline \end{array}$$

has rank $\binom{v}{t}$ *over every field, and* (ii) *the module generated by the rows of* W_{tk} *is equal to that generated by the rows of*

$$\bigsqcup_{j=0}^{t} \binom{k-j}{t-j} E_{jt}.$$

Proof. This is a somewhat more general form of Lemma 2 in [9]. The proof of part (ii) here is exactly the same as in the proof in [9] (although, perhaps confusingly, there is a different use of the symbols j, t, k there). The hypothesis $v \geq 2k$ of Lemma 2 of [9] is not really used; all that is required is that $t \leq k \leq v - t$.

We need to prove part (i) however, as the proof of Lemma 2 in [9] does use the hypothesis $v \geq 2k$. Perhaps the quickest way to derive part (i) is to use the fact, proved in [8], that when $t \leq k \leq v - t$, the matrix $\bigsqcup_{j=0}^{t} W_{jk}$ has rank $\binom{v}{t}$ over every field. The matrix $\bigsqcup_{j=0}^{t} E_{jk}$ has $\binom{v}{t}$ rows and so has rank at most $\binom{v}{t}$ over any field. Its row-module $\mathcal{M}$ contains the row-module of the matrix $\bigsqcup_{i=0}^{j} \binom{k-i}{j-i} E_{ik}$, which by part (ii) is the row-module of W_{jk}; so $\mathcal{M}$ contains the row-module of $\bigsqcup_{j=0}^{t} W_{jk}$ and thus has rank at least $\binom{v}{t}$ over every field. □

The proof of the following extension of Lemma 6 is essentially the same as the induction step in the proof of Lemma 2 of [9]. But as it may not be entirely clear what we mean, we repeat the proof here.

Lemma 7. *Let* v *be a positive integer,* ℓ *any integer, and* p *a prime. Let* $\mathcal{F}$ *be a family of subsets of a* v*-set* X *such that* $|A| \equiv \ell \pmod p$ *for every* $A \in \mathcal{F}$*, and let* N_j *denote the* j*-th inclusion matrix of* $\mathcal{F}$*. For* $0 \leq j < p$*, there exists a matrix* L_j *that consists of* $\binom{v}{j} - \binom{v}{j-1}$ *rows of* N_j *and such that for any* $t < p$*,*

$$\operatorname{row}_p(N_t) = \operatorname{row}_p\left(\bigsqcup_{i=0}^{t} \binom{\ell-i}{t-i} L_i\right). \tag{5}$$

In particular, the row spaces over F_p *of* $N_0, N_1, \ldots, N_s$ *are all contained in* $\operatorname{row}_p\left(\bigsqcup_{j=0}^{s} L_j\right)$*, which has dimension at most* $\binom{v}{s}$*.*

Proof. If all members of $\mathcal{F}$ have size k, then

$$W_{ij}N_j = \binom{k-i}{j-i} N_i. \tag{6}$$

If all members of $\mathcal{F}$ have size $\equiv \ell \pmod p$, we can still say

$$W_{ij}N_j \equiv \binom{\ell-i}{j-i} N_i \pmod p. \tag{7}$$

This is because the entry in row I and column A of $W_{ij}N_j$ is the number of j-subsets of X that contain I but which are contained in A. This is 0 unless $I \subseteq A$, in which case it is $\binom{|A|-i}{j-i}$.

For $i \leq j \leq v - i$, a family $\mathcal{B}$ of j-subsets of a v-set is called an (i, j)*-basis* when the columns of W_{ij} indexed by $\mathcal{B}$ provide a basis for the module over the integers generated by the entire set of columns of W_{ij}. Such a basis exists and examples are given explicitly in several sources; see e.g. [5,9].

Let L_0 be N_0 (a matrix with one row of all 1's) and for $i > 0$, let L_i be obtained by deleting from the matrix N_i the rows indexed by an $(i-1, i)$-basis.

By (7), $\operatorname{row}_p\left(\binom{\ell-i}{t-i} L_i\right) \subseteq \operatorname{row}_p(N_t)$ for any $i \leq t$, so the right-hand side of (5) is contained in the right-hand side. We prove the reverse containment by induction on t. It is trivially true when $t = 0$. Assume (5) is valid when t is replaced by any s, $s < t$.

Let $F = \bigsqcup_{i=0}^{t-1} E_{it}$, where the matrices E_{it} are as in Lemma 6. Then

$$\begin{aligned} \operatorname{row}_p(FN_t) &= \operatorname{row}_p\left(\bigsqcup_{i=0}^{t-1} E_{it}N_t\right) \\ &\subseteq \operatorname{row}_p\left(\bigsqcup_{i=0}^{t-1} W_{it}N_t\right) \subseteq \operatorname{row}_p\left(\bigsqcup_{i=0}^{t-1} \binom{\ell-i}{t-i} N_i\right). \end{aligned}$$

By the induction hypothesis applied to $N_0, N_1, \ldots, N_{t-1}$, the last expression above is equal to

$$\operatorname{row}_p\left(\bigsqcup_{i=0}^{t-1} \bigsqcup_{a=0}^{i} \binom{\ell-a}{i-a} \binom{\ell-i}{t-i} L_a\right),$$

and since $\binom{\ell-a}{i-a}\binom{\ell-i}{t-i} = \binom{\ell-a}{t-a}\binom{t-a}{i-a}$, we have

$$\mathrm{row}_p\,(FN_t) \subseteq \mathrm{row}_p\left(\bigsqcup_{a=0}^{t-1}\binom{\ell-a}{t-a}L_a\right). \tag{8}$$

Let C be the matrix consisting of the $\binom{v}{t-1}$ rows, corresponding to a $(t-1,t)$-basis $\mathcal{B}$, that were deleted from N_t to obtain L_t. For notational convenience, we may order the rows of N_t so that

$$N_t = \begin{array}{|c|}\hline C \\ \hline L_t \\ \hline \end{array}$$

Write

$$F := \bigsqcup_{i=0}^{t-1} E_{it} = \begin{array}{|c|c|}\hline U & V \\ \hline \end{array}$$

where the columns of U are those labeled by t-subsets in $\mathcal{B}$. It is shown in the proof of Lemma 2 in [9] that U is unimodular. We have $FN_t = UC + VL_t$, and from (8),

$$\mathrm{row}_p\,(UC) \subseteq \mathrm{row}_p\,(FN_t) + \mathrm{row}_p\,(VL_t) \subseteq \mathrm{row}_p\left(\bigsqcup_{a=0}^{t}\binom{k-a}{t-a}L_a\right). \tag{9}$$

Since U is nonsingular modulo p, $\mathrm{row}_p\,(UC) = \mathrm{row}_p\,(C)$. Recall that $N_t = C \bigsqcup L_t$. Since both $\mathrm{row}_p\,(C)$ and $\mathrm{row}_p\,(L_t)$ are contained in the right-hand side of (9), so is $\mathrm{row}_p\,(N_t)$. □

3. The case of equality in Theorem 3

Assume the hypotheses of Theorem 3 hold for some family $\mathcal{F}$ of k-subsets of a v-set. The polynomial f can be multiplied by an integer prime to p without changing the hypotheses, and it will be convenient to assume that $f(k) \equiv 1 \pmod p$. From (4) and (6),

$$P = N_s^{\top} C N_s \quad \text{where } C = \sum_{i=0}^{s} \frac{c_i}{\binom{k-i}{s-i}^2} W_{is}^{\top} W_{is},$$

and P is an integer matrix that is congruent modulo p to the identity matrix. We must consider this as an equation over the rationals, since p may divide some of the denominators of the coefficients in the expression for C. The matrices N_s and C above are also square of order $\binom{v}{s}$ and are nonsingular over the rationals (since P is).

The rational matrix C is in the Bose–Mesner algebra (over the rationals) $\mathcal{A}$ of the Johnson scheme $J(v,k)$; see [2] or [6](Ch. 30). This algebra consists of all matrices M with rows and columns indexed by the k-subsets of a v-set so that the entry in row A and column B depends only on the cardinality of $A \cap B$. Since $C \in \mathcal{A}$, its inverse C^{-1} is also in $\mathcal{A}$ (the inverse of a matrix is a polynomial in that matrix).

Let $m = \det(P)$. Since P is an integer matrix, mP^{-1} is an integer matrix (by e.g. Cramer's Rule). We have

$$N_s P^{-1} N_s^{\top} = C^{-1}, \qquad N_s(mP^{-1})N_s^{\top} = mC^{-1},$$

where in the equation on the right, the matrices N_s and mP^{-1} are integer matrices, and hence so is mC^{-1}. Since $P \equiv I \pmod p$, $m \equiv 1 \pmod p$ and

$$N_s N_s^{\top} \equiv mC^{-1} \pmod p.$$

The entry in row S and column T of $N_s N_s^{\top}$ is $\lambda(S \cup T)$, and this is congruent modulo p to a function $h(|S \cap T|)$ of $|S \cap T|$. If Y is a d-subset of X with $s \le d \le 2s$, we can choose s-subsets S and T so that $S \cup T = Y$. Then $\lambda(Y) = \lambda(S \cup T) = h(2s-d)$ and this is the same value for all d-subsets Y. □

4. Existence of p-ary t-designs

In this section, we think of a p-ary t-design as an integer vector $\mathbf{x}$ over F_p with coordinates indexed by the k-subsets of a v-set X so that

$$\boxed{W_{tk}}\ \boxed{\mathbf{x}} \equiv \lambda \boxed{1} \pmod{p} \tag{10}$$

for some integer λ. Of course, the coordinates of $\mathbf{x}$ can be adjusted modulo p without affecting (10); for example, we can make them all nonnegative. If the entries of $\mathbf{x}$ are nonnegative integers, the family of k-subsets where A has multiplicity equal to the entry of $\mathbf{x}$ in position A will be a p-ary t-(v, k, λ) design as defined in Section 1 if and only if (10) holds.

We say $\mathbf{x}$ is a *simple* p-ary t-design when $\mathbf{x}$ is a $(0, 1)$-vector. We say $\mathbf{x}$ is a *null* p-ary t-design when $\lambda = 0$. Nonzero null p-ary t-designs exist whenever $t < k \le v - t$, because then W_{tk} has more columns than rows. It is known (it follows from the Chevalley–Warning Theorem; or see [11]) that a homogeneous system of m linear equations over F_p in more than $m(p-1)$ variables has a nonzero solution in 0's and 1's, and thus we have the following theorem.

Theorem 8. *If* $\binom{v}{k} > (p-1)\binom{v}{t}$, *then there exist nonzero simple null* p*-ary* t*-designs with blocks of size* k.

Let t, k, and v be given. The relation

$$W_{jt}W_{tk} = \binom{k-j}{t-j} W_{jk}$$

is fundamental. We note that if $\mathbf{x}$ is a p-ary t-design and j is such that

$$\binom{k-j}{t-j} \not\equiv 0 \pmod{p},$$

then $\mathbf{x}$ is also a j-design. This is because

$$\binom{k-j}{t-j} W_{jk}\mathbf{x} = W_{jt}W_{tk}\mathbf{x} \equiv \lambda W_{jt}1 \equiv \lambda \binom{v-j}{t-j} 1 \pmod{p}.$$

But if

$$\binom{k-j}{t-j} \equiv 0 \pmod{p},$$

then there are examples of p-ary t-designs that are not p-ary j-designs:

Theorem 9. *Let* $t \le k \le v - t$ *be given and let* p *be a prime. Then there exists a null* p*-ary* t*-design* $\mathbf{x}$ *which fails to be a* j*-design for every* $j > 0$ *with* $\binom{k-j}{t-j} \equiv 0 \pmod{p}$.

Proof. Let the matrices E_{ik} be as in Lemma 6. The rows of $\bigsqcup_{j=0}^{t} E_{ik}$ are linearly independent over F_p, so for any $\mathbf{z}$ of height $\binom{v}{t}$ we can solve $(\bigsqcup_{j=0}^{t} E_{ik})\mathbf{x} \equiv \mathbf{z} \pmod{p}$. Choose $\mathbf{x}$ so that $E_{ik}\mathbf{x} \equiv \mathbf{0} \pmod{p}$ for i such that $\binom{k-i}{t-i} \not\equiv 0 \pmod{p}$, but $E_{jk}\mathbf{x}$ has at least two different coordinates modulo p when $\binom{k-j}{t-j} \equiv 0 \pmod{p}$. Since $E_{jk} \subseteq W_{jk}$, in the latter case $W_{jk}\mathbf{x}$ has at least two different coordinates. Since the row space of W_{tk} is that of $\bigsqcup_{i=0}^{t} \binom{k-i}{t-i} E_{ik}$, $W_{tk}\mathbf{x} \equiv \mathbf{0} \pmod{p}$. □

The existence questions for nonnull p-ary t-designs is settled completely in [10], where the following is proved in the discussion preceding Lemma 5 of [10].

Theorem 10. *Let* $t \le k \le v - t$. *Then there exists an integer vector* $\mathbf{x}$ *so that* $W_{tk}\mathbf{x} \equiv 1 \pmod{p}$ *if and only if*

$$\binom{k-i}{t-i} \equiv 0 \pmod{p} \quad \textit{implies} \quad \binom{v-i}{t-i} \equiv 0 \pmod{p}.$$

5. Fisher-like inequalities for p-ary t-designs

For a classical $2s$-(v, k, λ)-design with block set $\mathcal{F}$, the inequality $|\mathcal{F}| \ge \binom{v}{s}$ holds as long as $s \le k \le v - s$; see [6] (Theorem 19.8).

This inequality fails dramatically for p-ary t-designs. As an example, consider the incidence structure $\mathcal{S} = \mathcal{S}(n, k)$ whose points are the points of the projective geometry $PG(n, q)$ of dimension n over the field of q elements, where $q = p^e$ is a power of a prime p, and whose blocks are the (sets of points on) the subspaces of projective dimension k, $1 \le k \le n$. If $n \ge k(t-1)/t$, then the intersection of any t of these subspaces is nontrivial and so has cardinality $1 + q + \cdots + q^r$ for some $r \ge 0$, which is $\equiv 1 \pmod{p}$. This means that the *dual* $\mathcal{S}^*$ of $\mathcal{S}$ is a p-ary t-design for all $t = 1, 2, \ldots, \lfloor n/k \rfloor$, always with $\lambda = 1$. The number of points of $\mathcal{S}^*$ is the Gaussian number $\begin{bmatrix} n \\ k \end{bmatrix}_q$ while the number of blocks is only $\begin{bmatrix} n \\ 1 \end{bmatrix}_q$.

Under additional hypotheses, one can give substantial lower bounds on the number of blocks of a p-ary t-design.

For the rest of this section, let $(X, \mathcal{A})$ be a p-ary $\{s, s+1, \ldots, 2s\}$-design with blocks of size k and $v = |X| \ge 2s$. Let λ_t^0 be the number, modulo p, of blocks that contain a t-subset of points for $t \in \{s, s+1, \ldots, 2s\}$ and define λ_j^i, modulo p, for

$s \le j \le 2s - i$ recursively by $\lambda_j^i = \lambda_j^{i-1} - \lambda_{j+1}^{i-1}$. The combinatorial interpretation of λ_j^i is the number, modulo p, of blocks that contain all of a set of j points and none of a set of i other points; this may be proved by induction on i.

Theorem 11. *If* $\lambda_s^s \not\equiv 0 \pmod p$, *then*

$$|\mathcal{F}| \ge \sum_{i \in Q} \left(\binom{v}{i} - \binom{v}{i-1} \right) \ge \binom{v}{s} - \binom{v}{s-1}, \tag{11}$$

where Q *is the set of indices* i, $0 \le i \le s$, *such that*

$$\binom{v-s-i}{s-i} \not\equiv 0 \pmod p$$

and where we understand $\binom{v}{-1}$ *as zero.*

Proof. Let $\overline{N}_i$ devote the i-th *disjointness matrix* defined by

$$\overline{N}_i(I, A) = \begin{cases} 1 & \text{if } I \cap A = \emptyset, \\ 0 & \text{otherwise.} \end{cases}$$

Here I is an i-subset of X and $A \in \mathcal{F}$. We have

$$N_s \overline{N}_s^{\top} \equiv \lambda_s^s \overline{W}_{ss} \pmod p$$

where $\overline{W}_{ss}$ is the s-th disjointness matrix for the family of all s-subsets of X. We may identify $\overline{W}_{ss}$ with $W_{s,v-s}$, because one s-subset is disjoint from another if and only if the first is contained in the complement of the second. By Lemma 6, the p-rank of $W_{s,v-s}$ is the quantity in the middle of (11). This quantity cannot exceed the columns of N_s, which is $|\mathcal{F}|$. □

This bound may be improved if we know $\lambda_s^j \not\equiv 0 \pmod p$ for other values of j. For $j = 0, 1, \ldots, s$, we have

$$N_s \overline{N}_j \equiv \lambda_s^j \overline{W}_{sj} \equiv \lambda_s^j W_{j,v-s}^{\top} \sim \left(\bigsqcup_{i=0}^{j} \binom{v-j-i}{j-i} E_{i,v-s} \right)^{\top} \pmod p,$$

where the matrices $E_{i,v-s}$ are as in Lemma 6 and the "$\sim$" means "has the same row space over F_p as". So $\mathrm{row}_p\left(E_{i,v-s}\right)$ is contained in the column space of N_s over F_p whenever $i \in Q'$, the set of indices i, $0 \le i \le s$, such that for some j, $i \le j \le s$,

$$\lambda_s^j \binom{v-j-i}{j-i} \not\equiv 0 \pmod p,$$

and the inequality (11) holds when Q is replaced by the possibly larger set Q'.

Acknowledgement

The author's research was supported by NSA Grant H98230-04-1-0037.

References

[1] L. Babai, P. Frankl, S. Kutin, S. Štefankovič, Set Systems with restricted intersections modulo prime powers, J. Combin. Theory, Ser. A 95 (2001) 39–73.
[2] Ph. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Rep. (Suppl. 10) (1973).
[3] P. Frankl, R.M. Wilson, Intersection theorems with geometric consequences, Combinatorica 1 (1981) 357–368.
[4] P. Keevash, D. Mubayi, R.M. Wilson, Set systems with no singleton intersection, SIAM J. Discrete. Math. 20 (2006) 1031–1041.
[5] G.B. Khosrovshahi, S. Adjoodani-Namini, A new basis for trades, SIAM J. Discrete. Math. 3 (1990) 364–372.
[6] J.H. van Lint, R.M. Wilson, A Course in Combinatorics, 2nd edition, Cambridge University Press, Cambridge, 2001.
[7] D.K. Ray-Chaudhuri, R.M. Wilson, On t-designs, Osaka J. Math. 12 (1975) 737–744.
[8] R.M. Wilson, A diagonal form for the incidence matrices of t-subsets vs. k-subsets, European J. Combin. 11 (1990) 609–615.
[9] R.M. Wilson, Signed hypergraph designs and diagonal forms for some incidence matrices, Des. Codes Cryptogr. 17 (1999) 289–297.
[10] R.M. Wilson, Some applications of incidence matrices of t-subsets and hypergraphs, in: For the Proceedings of the Fourth Shanghai Conference on Combinatorics, Discrete Math. (2002) (to appear).
[11] R.M. Wilson, An Ax-Katz-type theorem for congruences modulo powers of a prime, J. Number Theory (submitted for publication).